UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/806,020	03/22/2004	Andrew D. Birrell	MSFT-5310/307233.01	1990

41505 7590 10/29/2008

WOODCOCK WASHBURN LLP (MICROSOFT CORPORATION)
CIRA CENTRE, 12TH FLOOR
2929 ARCH STREET
PHILADELPHIA, PA 19104-2891

EXAMINER	
PAN, JOSEPH T	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
10/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/806,020	BIRRELL ET AL.	
	Examiner	Art Unit	
	JOSEPH PAN	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 July 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-10,12-20,28-34 and 38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-10,12-20,28-34 and 38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's response filed on July 29, 2008 has been carefully considered. Claims 1, 12, 28, and 36 have been amended. Claims 1, 3-10, 12-20, 28-34, and 36 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 3-10, 12-20, 28-34, and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Juels et al. (U.S. Patent No. 7,197,639 B1) in view of Landsman et al. (U.S. Pub. No. 2005/0055410 A1), hereinafter "Landsman".

Referring to claims 1, 28, 36:

i. Juels teaches:

A cancellation server of a digital delivery system, the cancellation server communicatively coupled to at least one database, and configured for executing the steps of:

communicatively coupling a cancellation server to at least one database comprising a plurality of unique identifiers for cryptographic puzzles (see

column 19, lines 38-47 of Juels);

receiving an identifier associated with a cryptographic puzzle, the puzzle being attached to a digital object, the digital object being an electronic mail message intended for delivery from a sender to a recipient distinct from the sender (see figure 2, element 270 'communicate verification of the correct results of the task'; column 19, lines 38-47 ' Note that to prevent an adversary from using the same solved puzzle for multiple allocations, the server 120 must ensure that only one slot in B is allocated for each request M.sub.i. One way to accomplish this is to let some unique identifier derived from M.sub.i.sup.1 [i.e., request] be associated with the slot allocated for M.sub.i. On receiving a correctly solved puzzle corresponding to M.sub.i, the server 120 checks that no slot has been allocated for it already. One means of enabling a rapid search for already-used identifiers would be to assign slots through bucket hashing on identifiers.'; column 7, line 59 – column 8, line 26; column 17, lines 59-65; and column 1, lines 39-47 "Other connection depletion attacks in this same genre include so-called "e-mail bomb" attacks, in which many thousands of **e-mail deliveries** are directed at a single server target.", of Juels);

Validating the identifier by verifying that the identifier does not exist in the at least one database (see column 16, lines 25-27 'In an another embodiment, the server 120 does not accept more than one or more than a limited number of solutions to a particular puzzle from a client 110.', of Juels); and

Upon validating, canceling the cryptographic puzzle and storing in at least one database, an entry comprising the identifier or information derived from the identifier, and transmitting an ACCEPT response if the identifier is validated (see figure 2, element 280 'validate verification of the correct results of the task'; column 19, lines 38-47; column 7, line 59 – column 8, line 26; and figure 5, element 330 'positive response to the query' [i.e., ACCEPT], element 295 'communicate negative resource allocation acknowledgment' [i.e., REJECT], of Juels).

Juels disclose searching for already-used identifiers in a database [i.e., "bucket hashing on identifiers"]. However, Juels does not specifically using the

term database. Neither does Juels specifically mention transmitting the response from the server to the recipient distinct from the sender.

ii. Landsman teaches a method of managing electronic messages wherein Landsman discloses the database (see page 4, paragraph [0042] of Landsman).

Landsman further discloses transmitting the message from the server to the recipient distinct from the sender (see figure 1A, element 16 'recipient server', 12 'recipient computer'; and figure 5, element 70 'deliver message', of Landsman).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Landsman into the method of Juels to couple the cancellation server to a database.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Landsman into the method of Juels to be able to send a message from the server to a recipient distinct from the sender.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Landsman into the system of Juels to couple the cancellation server to a database, because it's well known in the art that the database can store and keep track of information. Therefore Landsman's teaching could enhance Juels's system.

The ordinary skilled person would have been motivated to have applied the teaching of Landsman into the system of Juels to be able to send a message from the server to a recipient distinct from the sender, because Juels discloses "In one embodiment, the invention relates to an apparatus for allocating a resource including a first receiver receiving a resource allocation request from a client, a puzzle generator creating a computational task for the client to perform, a transmitter communicating the computational task to the client, a second receiver receiving a verification that the client has correctly performed the computational task within a predetermined time limit, and an allocator allocating resources for the client." (see

column 3, lines 54-52 of Juels, emphasis added). Therefore Landsman's teaching could enhance Juels's system.

Referring to claim 3:

Juels and Landsman teach the claimed subject matter: a cancellation server for canceling cryptographic puzzles (see claim 1 above). They further disclose transmitting a response (see e.g. figure 5, element 295 'communicate negative response allocation acknowledgment' of Juels).

Referring to claims 4, 29:

Juels and Landsman teach the claimed subject matter: a cancellation server for canceling cryptographic puzzles (see claim 1 above). They further disclose the timestamp (see figure 8, element 510 'time stamp' of Juels).

Referring to claims 5, 30:

Juels and Landsman teach the claimed subject matter: a cancellation server for canceling cryptographic puzzles (see claim 1 above). They further disclose the range of values (see column 11, lines 46-57 of Juels).

Referring to claims 6, 34:

Juels and Landsman teach the claimed subject matter: a cancellation server for canceling cryptographic puzzles (see claim 1 above). They further disclose verifying that the identifier does not exist in the at least one database (see column 16, lines 25-27; and column 19, lines 38-47 of Juels).

Referring to claim 7:

Juels and Landsman teach the claimed subject matter: a cancellation server for canceling cryptographic puzzles (see claim 1 above). They further disclose the hashing (see column 3, lines 12-16 of Juels).

Referring to claims 8, 31:

Juels and Landsman teach the claimed subject matter: a cancellation server for canceling cryptographic puzzles (see claim 1 above). They further disclose the second server (see column 3, lines 54-62 of Juels).

Referring to claims 9, 32:

Juels and Landsman teach the claimed subject matter: a cancellation server for canceling cryptographic puzzles (see claim 1 above). They further disclose the database (see page 4, paragraph [0042], lines 3-8 of Landsman).

Referring to claims 10, 33:

Juels and Landsman teach the claimed subject matter: a cancellation server for canceling cryptographic puzzles (see claim 1 above). They further disclose the network (see column 2, lines 30 of Juels).

Referring to claim 12:

i. Juels teaches:

A puzzle checker for use in a digital delivery system , the puzzle checker communicatively coupled with a cancellation server, and configured for executing the steps of:

communicatively coupling a cancellation server to at least one database comprising a plurality of unique identifiers for cryptographic puzzles (see column 19, lines 38-47 of Juels);

transmitting to the cancellation server, an identifier associated with a cryptographic puzzle attached to a digital object, the digital object being an electronic mail message intended for delivery from a sender to a recipient distinct from the sender, the puzzle checker being associated with the recipient (see figure 2, element 270 'communicate verification of the correct results of the task'; column 19, lines 38-47 ' Note that to prevent an adversary from using the same solved puzzle for multiple allocations, the server 120 must ensure that only one slot in B is allocated for each request M.sub.i. One way to accomplish this is to let some unique identifier derived from M.sub.i.sup.1 [i.e., request] be associated with the slot allocated for M.sub.i. On receiving a correctly solved puzzle corresponding to M.sub.i, the server 120 checks that no slot has been allocated for it already. One means of enabling a rapid search for already-used identifiers would be to assign slots through bucket hashing on identifiers.'; column 7, line 59 – column 8, line 26; column 17, lines 59-65; , and column 1, lines 39-47 "Other connection depletion attacks in this same genre include so-called "e-mail bomb" attacks, in which many thousands of **e-mail deliveries** are directed at a single

server target,", of Juels, emphasis added); and

receiving a REJECT response from the cancellation server as a result of the identifier being already present in a database of the cancellation server (see figure 5, element 285 'reject verification of the correct results of the task'; and column 16, lines 25-27 'In an another embodiment, the server 120 does not accept more than one or more than a limited number of solutions to a particular puzzle from a client 110.', of Juels, emphasis added); and

Processing the digital object in response to receiving the REJECT response (see column 13, lines 31-45 of Juels).

Juels disclose searching for already-used identifiers in a database [i.e., "bucket hashing on identifiers"]. However, Juels does not specifically using the term database. Neither does Juels specifically mention transmitting the response from the server to the recipient distinct from the sender.

ii. Landsman teaches a method of managing electronic messages wherein Landsman discloses the database (see page 4, paragraph [0042] of Landsman).

Landsman further discloses transmitting the message from the server to the recipient distinct from the sender (see figure 1A, element 16 'recipient server', 12 'recipient computer'; and figure 5, element 70 'deliver message', of Landsman).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Landsman into the method of Juels to couple the cancellation server to a database.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Landsman into the method of Juels to be able to send a message from the server to a recipient distinct from the sender.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Landsman into the system of Juels to couple the cancellation server to a database, because it's well known in the art that the database can store and

keep track of information. Therefore Landsman's teaching could enhance Juels's system.

The ordinary skilled person would have been motivated to have applied the teaching of Landsman into the system of Juels to be able to send a message from the server to a recipient distinct from the sender, because Juels discloses "In one embodiment, the invention relates to an apparatus for allocating a resource including a first receiver receiving a resource allocation request from a client, a puzzle generator creating a computational task for the client to perform, a transmitter communicating the computational task to the client, a second receiver receiving a verification that the client has correctly performed the computational task within a predetermined time limit, and an allocator allocating resources for the client." (see column 3, lines 54-52 of Juels, emphasis added). Therefore Landsman's teaching could enhance Juels's system.

Referring to claim 13:

i. Juels teaches the claimed subject matter:

A puzzle checker for verifying solutions to cryptographic puzzles (see claim 12 above). However, Juels does not specifically mention removing the object.

ii. Landsman teaches a method of managing electronic messages wherein Landsman discloses the removing an object (see page 1, paragraph [0016], lines 8-10 of Landsman).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Landsman into the method of Juels to add the feature of removing an object.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Landsman into the system of Juels to add the feature of removing an object, because when the server rejects verification of the correct results of the task and communicate negative resource allocation acknowledgement to the client (see figure 5, elements 285, 295 of Juels), the original client's request (see figure 5,

element 230 'communicate resource allocation request of Juels) need to be removed from the server.

Referring to claim 14:

Juels and Landsman teach the claimed subject matter: a puzzle checker for verifying solutions to cryptographic puzzles (see claim 13 above). They further disclose the filtering (see page 1, paragraph [0010] of Landsman).

Referring to claim 15:

Juels and Landsman teach the claimed subject matter: a puzzle checker for verifying solutions to cryptographic puzzles (see claim 13 above). They further disclose the modification (see column 22, lines 8-11 Juels).

Referring to claim 16:

Juels and Landsman teach the claimed subject matter: a puzzle checker for verifying solutions to cryptographic puzzles (see claim 13 above). They further disclose verifying whether the solution solves the puzzle, and processing the object (see figure 2, elements 280 'validate verification of the correct results of the task', 290 'allocate resource and communicate resource allocation acknowledgment', of Juels).

Referring to claim 17:

Juels and Landsman teach the claimed subject matter: a puzzle checker for verifying solutions to cryptographic puzzles (see claim 13 above). They further disclose the timestamp (see figure 8, element 510 'time stamp' of Juels), and the threshold range of time (see column 13, lines 40-41 'within time T' of Juels).

Referring to claim 18:

Juels and Landsman teach the claimed subject matter: a puzzle checker for verifying solutions to cryptographic puzzles (see claim 13 above). They further disclose the hash of the identifier (see column 19, line 47 'hashing on identifiers', of Juels).

Referring to claims 19-20:

Juels and Landsman teach the claimed subject matter: a puzzle checker for verifying solutions to cryptographic puzzles (see claim 13 above). They further

disclose the recipient computer and the intermediate server (see figure 1A, element 12, 'recipient computer', 16 'recipient server' of Landsman).

Response to Arguments

4. Applicant's arguments filed on July 29, 2008 have been fully considered but they are not persuasive.

(1) Applicant argues:

"Juels and Landsman, whether considered separately or in combination, neither disclose nor suggest "communicatively coupling a cancellation server to at least one database comprising a plurality of unique identifiers for cryptographic puzzles" as recited in claims 1, 12, and 36, nor "communicatively connecting to at least one database comprising a plurality of unique identifiers for cryptographic puzzles" as recited in claim 28." (page 1, 4th paragraph, Applicant's Arguments/Remarks, emphasis added)

Examiner maintains:

Juels discloses "Note that to prevent an adversary from using the same solved puzzle for multiple allocations, the server 120 must ensure that only one slot in B is allocated for each request M.sub.i. One way to accomplish this is to let some unique identifier derived from M.sub.i.sup.1 be associated with the slot allocated for M.sub.i. On receiving a correctly solved puzzle corresponding to M.sub.i, the server 120 checks that no slot has been allocated for it already. One means of enabling a rapid search for already-used identifiers [i.e., search a plurality of unique identifies of cryptographic puzzles] would be to assign slots through bucket hashing on identifiers. [i.e., storing the plurality of unique identifiers in buckets through bucket hashing on identifiers]" (see column 19, lines 38-47 of Juels, emphasis added). Therefore, Juels discloses communicatively coupling or connecting a canellation server to bucket(s) [i.e., a

database] comprising a plurality of unique identifiers for cryptographic puzzles. However, Juels does not explicitly disclose the concept of database.

On the other hand, Landsman discloses "In response to the receipt of the incoming electronic message 40 from the sender, a challenge generation module 48 of a challenge module 42 of the recipient server 16 may determine whether the sender is designated in a sender database 56 as being authorized (or unauthorized) to send electronic messages to the recipient." (see page 4, paragraph [0042], lines 3-8 of Landsman). Therefore, Landsman discloses the concept of database.

Thus, the combination of Juels and Landsman disclose communicatively coupling a cancellation server to at least one database comprising a plurality of unique identifiers for cryptographic puzzles" as recited in claims 1, 12, and 36, nor "communicatively connecting to at least one database comprising a plurality of unique identifiers for cryptographic puzzles" as recited in claim 28.

(2) Applicant argues:

"The Office Action asserts that Juels teaches a cancellation server communicatively coupled to at least one database, however, it does not. The Office Action looks to Landsman for a disclosure of a database use, however, Landsman does not provide the remedy for the lack of disclosure in Jules." (page 2, 1st paragraph, Applicant's Arguments/Remarks)

Examiner maintains:

See Examiner's response in (1) above.

Conclusion

5. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is

not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph Pan whose telephone number is 571-272-5987.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

/Joseph Pan/
Examiner, Art Unit 2435
October 15, 2008
/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2431